

AMENDMENTS TO THE CLAIMS

1. (currently amended) A method comprising:

outputting, in a user interface configured to verify an identity of a single user for access to an identity integration system, one or more of a plurality of questions having answers that do not involve a user name or password of the single user;

if correct answers to the one or more questions are received via the user interface, outputting a user interface configured to interact with ~~thean~~ identity integration system to perform collective password management for multiple user accounts, each of the multiple user accounts being associated with ~~thea~~ single user;

receiving a selection of selecting multiple data sources connected to an the identity integration system input by the single user via the user interface, wherein [[::]] each of the multiple data sources corresponds to a different one of said multiple user accounts;

the identity integration system includes a management agent for each of the multiple data sources configured specifically for its respective data source to manage data communication between the identity integration system and each respective data source; and

-for at least some of the multiple data sources a management agent for the data source is configured with credentials to perform password management for a corresponding said user account;

receiving a new password input by the single user via the user interface; and

performing an administrative password operation on a-multiple passwords each associated with each one of the selected multiple data sources to collectively update each said of the multiple passwords to the new password, wherein the password operation is performed using the identity integration system.

2. (previously presented) The method as recited in claim 1, further comprising:

determining an identity of a the single user, wherein the multiple data sources are associated with the identity; and

querying the identity integration system to find the multiple data sources associated with the identity.

3. (original) The method as recited in claim 1, wherein the password operation comprises updating one or more passwords associated with the multiple data sources using joined objects across the multiple data sources, wherein the joined objects are stored in the identity integration system.

4. (original) The method as recited in claim 3, wherein some of the multiple passwords are updated to new passwords that differ from each other.

5. (original) The method as recited in claim 3, wherein each of the multiple passwords is updated to the same password.

6. (original) The method as recited in claim 1, wherein the password operation comprises one of changing, setting and resetting the password.

7. (original) The method as recited in claim 1, wherein each of the multiple data sources differ from others of the multiple data sources with respect to at least one of a protocol, a platform, a format, and a data transmission medium for data storage.

8. (original) The method as recited in claim 1, wherein each of the multiple data sources differs in a connection to the identity integration system with respect to at least one of a protocol, a platform, a format, and a data transmission medium for data storage.

9. (original) The method as recited in claim 1, wherein each of the multiple data sources uses a different password management function.

10. (original) The method as recited in claim 9, wherein the identity integration system performs password management for each of the multiple data sources.

11. (original) The method as recited in claim 1, wherein for at least some of the multiple data sources the identity integration system stores integrated identity information to perform password management.

12-14. (canceled).

15. (original) The method as recited in claim 1, further comprising using the identity integration system to produce a list of user accounts associated with the multiple data sources, wherein the user accounts on the list are eligible for password management.

16. (original) The method as recited in claim 1, further comprising allowing access to the identity integration system through a web application for password management.

17. (original) The method as recited in claim 16, wherein the selecting multiple data sources and the performing a password operation are performed on a website generated by the web application.

18. (previously presented) The method as recited in claim 17, wherein the web application accepts a password credential from the single user to perform the password operation.

19. (previously presented) The method as recited in claim 17, wherein the web application verifies an identity of the single user by asking the single user questions, wherein if answers provided by the single user are correct then the web application performs the password operation using the identity of a privileged user account.

20. (original) The method as recited in claim 17, further comprising using the identity integration system to produce a list of user accounts displayable on the website, wherein the user accounts are associated with the multiple data sources.

21. (original) The method as recited in claim 17, further comprising a help desk to at least assist in the performing a password operation.

22. (original) The method as recited in claim 17, further comprising communicatively coupling the identity integration system with the web application using an interface.

23. (original) The method as recited in claim 22, wherein the interface is publicly available.

24. (original) The method as recited in claim 22, wherein the interface allows a web application designer to customize the web application.

25. (original) The method as recited in claim 22, wherein the interface includes password management functions.

26. (original) The method as recited in claim 22, wherein the interface is capable of being changed for an improved version of the interface that adds more password management functions while using the same web application and the same identity integration system.

27. (cancelled).

28. (currently amended) The method as recited in claim 127, wherein the interface is secured using a security group.

29. (original) The method as recited in claim 28, wherein the interface is secured using a security group that allows both searching for a connector object associated with a data source and setting a password for an object in the data

source, wherein a connector object represents at least part of the data source in the identity integration system.

30. (previously presented) The method as recited in claim 1, wherein an identity of the single user associated with the multiple data sources provides a security credential for performing a password operation.

31. (previously presented) The method as recited in claim 17, wherein the web application produces a list of accounts associated with the single user.

32. (original) The method as recited in claim 31, wherein the web application lists only accounts eligible for password management.

33. (original) The method as recited in claim 17, wherein the web application adopts a web application behavior based on a configuration setting.

34. (original) The method as recited in claim 33, wherein the configuration setting is stored in a configuration file.

35. (original) The method as recited in claim 17, wherein the web application checks if one of the data sources is communicating before updating a password associated with the data source.

36. (original) The method as recited in claim 35, wherein the updating comprises one of changing and setting the password.

37. (original) The method as recited in claim 17, wherein the web application checks if a connection to one of the data sources is secure before updating a password associated with the data source.

38. (original) The method as recited in claim 37, wherein the updating comprises one of changing and setting the password.

39. (original) The method as recited in claim 1, further comprising displaying a status for the password operation.

40. (original) The method as recited in claim 39, further comprising displaying the status on a webpage.

41. (original) The method as recited in claim 1, further comprising auditing the password operation.

42. (original) The method as recited in claim 41, further comprising maintaining a password management history for the password operation.

43. (original) The method as recited in claim 42, further comprising keeping the password management history in a connector space object, wherein the connector space object is included in the identity integration system.

44. (original) The method as recited in claim 42, wherein the password management history includes a tracking identifier to an audit record of the password operation.

45. (original) The method as recited in claim 41, further comprising maintaining a repository of audit records for password operations performed using the identity integration system.

46. (previously presented) The method as recited in claim 45, wherein an audit record for a password operation includes at least one of an identifier of the single user associated with the password operation, a tracking identifier to a web application initiating the password operation, a tracking identifier to a connector object associated with the password operation, a tracking identifier to a management agent associated with the password operation, a password operation identifier, a password operation status, a date, and a time.

47. (original) The method as recited in claim 1, further comprising associating custom logic with a password operation, wherein the custom logic is executed after the password operation is performed.

48. (original) The method as recited in claim 47, wherein the custom logic sends an email.

49. (original) The method as recited in claim 47, wherein the custom logic logs password management activity.

50. (original) The method as recited in claim 47, wherein the custom logic performs a password operation on a subsequent data source not connected to the identity integration system.

51. (original) The method as recited in claim 1, wherein the password operation further comprises updating passwords in both secure and non-secure data sources within the multiple data sources.

52. (original) The method as recited in claim 1, wherein the password operation further comprises updating passwords over both secure and non-secure connections to the multiple data sources.

53. (currently amended) An apparatus comprising:

a processor; and

a web application for password management executable on the processor having one or more modules including:

a user identifier to find identity information in an identity integration system that corresponds to a single user, wherein:

~~the identity integration system includes a management agent for each of multiple data sources to manage data communication between the identity integration system and each respective data source; and~~

~~for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source;~~

identity information query logic to search information in the identity integration system for accounts associated with the single user;

an account lister to display the accounts associated with the single user;

an account selector to designate at least some of the displayed accounts for password management;

a password inputter to determine a new password input by the single user to associate with each designated accounts; and

a password manager to collectively manage passwords for the designated accounts that correspond to the single user by requesting an update of a password associated with each designated account to the new password, responsive to the user input, the update performed if correct answers to one or more questions are received via a user interface that are output in an event of a lost password to access the web application.

54. (previously presented) The apparatus as recited in claim 53, wherein the identity integration system connects with diverse data sources, each data source having a different function for using password security.

55. (previously presented) The apparatus as recited in claim 53, further comprising an account status display to show selected accounts and a connection status of each account.

56. (previously presented) The apparatus as recited in claim 53, further comprising a password management status display to display a password management operation status for each account.

57. (previously presented) The apparatus as recited in claim 53, further comprising a status checker to verify connectivity and security of a connection between an account and the identity integration system.

58. (previously presented) The apparatus as recited in claim 53, further comprising a configuration reader to obtain behavior settings for the web application.

59. (previously presented) The apparatus as recited in claim 53, further comprising a custom logic executor to perform custom logic associated with a password management operation.

60. (previously presented) The apparatus as recited in claim 53, wherein the account lister lists accounts eligible for password management and does not list accounts that are not eligible for password management.

61. (currently amended) An apparatus comprising a processor coupled to memory, the memory storing one or more modules executable via the processor to implement:

an interface for coupling an identity integration system with a password management web application;

logic for communicating with the identity integration system, wherein:

the identity integration system is capable of collectively updating a password on multiple data sources that use various functions of password updating responsive to input of a single new password by a single user, the identity integration system including a lost password feature that is selectable to provide one or more of a plurality of questions having answers that were previously supplied by the single user;

each said data source includes a user account that corresponds to the single user;

the identity integration system includes a management agent for each of the multiple data sources to manage data communication between the identity integration system and each respective data source; and

for at least some of the multiple data sources a management agent for the data source is configured with to obtain credentials from the single user to perform password management so that the credentials are not stored beforehand by the identity integration system;

logic for communicating with the password management web application;

logic for searching for objects in the identity integration system; and
logic for checking a connection status between the identity integration
system and a data source.

62. (previously presented) The apparatus as recited in claim 61, further
comprising logic for checking security of a connection between the identity
integration system and a data source.

63. (previously presented) The apparatus as recited in claim 61, further
comprising logic to change a password associated with the data source.

64. (previously presented) The apparatus as recited in claim 61, further
comprising logic to set a password associated with the data source.

Claims 65-85. (Canceled)